# Prácticas recomendadas y recomendaciones

Astra Trident

NetApp
April 16, 2024

# Tabla de contenidos

# Prácticas recomendadas y recomendaciones

## Puesta en marcha

Utilice las recomendaciones que se enumeran aquí cuando ponga en marcha Astra Trident.

### Póngalo en marcha a un espacio de nombres dedicado

"Espacios de nombres" proporcione separación administrativa entre distintas aplicaciones y una barrera para el uso compartido de recursos. Por ejemplo, una RVP de un espacio de nombres no se puede consumir de otro. Astra Trident proporciona recursos PV a todos los espacios de nombres en el clúster de Kubernetes y, por lo tanto, aprovecha una cuenta de servicio con privilegios elevados.

Además, el acceso al pod de Trident puede permitir a un usuario acceder a las credenciales del sistema de almacenamiento y a otra información confidencial. Es importante asegurarse de que los usuarios de aplicaciones y aplicaciones de gestión no tengan la capacidad de acceder a las definiciones de objetos de Trident o a los pods mismos.

### Utilice cuotas y límites de rango para controlar el consumo de almacenamiento

Kubernetes cuenta con dos funciones que, al combinarse, ofrecen un potente mecanismo que limita el consumo de recursos que consumen las aplicaciones. La "mecanismo de cuotas de almacenamiento" permite al administrador implementar límites de consumo globales, específicos para las clases de almacenamiento, de capacidad y de recuento de objetos en función del espacio de nombres. Además, utilizando un "límite de rango" Garantiza que las solicitudes de PVC se encuentren dentro de un valor mínimo y máximo antes de reenviar la solicitud al aprovisionador.

Estos valores se definen por espacio de nombres, lo que significa que cada espacio de nombres debe tener valores definidos que se ajustan a los requisitos de sus recursos. Consulte aquí para obtener más información acerca de "cómo aprovechar las cuotas".

## Configuración del almacenamiento

Cada plataforma de almacenamiento de la cartera de NetApp tiene unas funciones únicas que benefician a las aplicaciones, en contenedores o no.

### Descripción general de la plataforma

Trident funciona con ONTAP y Element. No existe una plataforma que se adapte mejor a todas las aplicaciones y escenarios que otra, sin embargo, las necesidades de la aplicación y el equipo que administra el dispositivo deben tenerse en cuenta al elegir una plataforma.

Debe seguir las prácticas recomendadas de base para el sistema operativo del host con el protocolo que está aprovechando. Opcionalmente, es posible que desee considerar la incorporación de prácticas recomendadas para las aplicaciones, cuando esté disponible, con configuración de back-end, clase de almacenamiento y RVP para optimizar el almacenamiento para aplicaciones específicas.

## Prácticas recomendadas para ONTAP y Cloud Volumes ONTAP

Conozca las prácticas recomendadas para configurar ONTAP y Cloud Volumes ONTAP para Trident.

Las siguientes recomendaciones son directrices para configurar ONTAP para cargas de trabajo en contenedores, que consumen volúmenes aprovisionados de forma dinámica por Trident. Cada uno de ellos debe considerarse y evaluarse según la idoneidad de su entorno.

### Utilice SVM dedicadas a Trident

Las máquinas virtuales de almacenamiento (SVM) proporcionan separación de tareas administrativas y de aislamiento entre clientes en un sistema ONTAP. Dedicar una SVM a las aplicaciones permite delegar privilegios y aplicar prácticas recomendadas para limitar el consumo de recursos.

Existen varias opciones disponibles para la gestión de la SVM:

- Proporcione la interfaz de gestión del clúster en la configuración del back-end, junto con las credenciales adecuadas, y especifique el nombre de la SVM.
- Cree una interfaz de gestión dedicada para la SVM mediante ONTAP System Manager o la CLI.
- Comparta la función de gestión con una interfaz de datos NFS.

En cada caso, la interfaz debe estar en DNS, y se debe usar el nombre DNS al configurar Trident. Esto permite facilitar algunas situaciones de recuperación ante desastres, por ejemplo, SVM-DR sin retención de identidad de red.

No tiene ninguna preferencia entre tener una LIF de gestión dedicada o compartida para la SVM, sin embargo, debe asegurarse de que las políticas de seguridad de red se alineen con el enfoque que elija. Sin embargo, debería accederse a la LIF de gestión a través de DNS para facilitar la máxima flexibilidad que debería tener "SVM-DR" Se podrá usar en combinación con Trident.

### Limite el número máximo de volúmenes

Los sistemas de almacenamiento de ONTAP tienen un número máximo de volúmenes, que varía en función de la versión del software y la plataforma de hardware. Consulte "Hardware Universe de NetApp" Para su plataforma y versión de ONTAP específica, determine los límites exactos. Cuando se agota el número de volúmenes, las operaciones de aprovisionamiento fallan no solo para Trident, sino para todas las solicitudes de almacenamiento.

De Trident `ontap-nas` y.. `ontap-san` Los controladores aprovisionan un FlexVolume para cada volumen persistente (PV) de Kubernetes que se crea. La `ontap-nas-economy` El controlador crea aproximadamente un FlexVolume por cada 200 VP (configurable entre 50 y 300). La `ontap-san-economy` El controlador crea aproximadamente un FlexVolume por cada 100 VP (configurable entre 50 y 200). Para evitar que Trident consuma todos los volúmenes disponibles en el sistema de almacenamiento, debe establecer un límite en la SVM. Puede hacerlo desde la línea de comandos:

```
vserver modify -vserver <svm_name> -max-volumes <num_of_volumes>
```

Valor para `max-volumes` varía en función de varios criterios específicos de su entorno:

- El número de volúmenes existentes en el clúster de ONTAP
- El número de volúmenes que espera aprovisionar fuera de Trident para otras aplicaciones

- El número de volúmenes persistentes que tienen previsto consumir las aplicaciones de Kubernetes

La `max-volumes` El valor es el total de volúmenes aprovisionados en todos los nodos del clúster de ONTAP, no en un nodo ONTAP individual. Como resultado, es posible que encuentre algunas condiciones en las que un nodo de un clúster de ONTAP pueda tener muchos más o menos volúmenes aprovisionados de Trident que otro nodo.

Por ejemplo, un clúster ONTAP de dos nodos tiene la capacidad de alojar un máximo de 2000 FlexVolumes. Tener el recuento de volumen máximo establecido en 1250 parece muy razonable. Sin embargo, si solo "agregados" De un nodo se asigna a la SVM, o los agregados asignados de un nodo no se pueden aprovisionar con (por ejemplo, debido a capacidad), el otro nodo se convierte en el destino para todos los volúmenes aprovisionados de Trident. Esto significa que es posible alcanzar el límite de volumen para ese nodo antes que el `max-volumes` Se alcanza el valor, lo que repercute tanto en Trident como en otras operaciones de volúmenes que utilizan ese nodo. **Puede evitar esta situación asegurándose de que los agregados de cada nodo del clúster están asignados a la SVM que utiliza Trident en los mismos números.**

#### Limite el tamaño máximo de los volúmenes que ha creado Trident

Para configurar el tamaño máximo de los volúmenes que Trident puede crear `limitVolumeSize` parámetro en la `backend.json` definición.

Además de controlar el tamaño del volumen en la cabina de almacenamiento, también se deben aprovechar las capacidades de Kubernetes.

#### Configure Trident para utilizar CHAP bidireccional

Puede especificar los nombres de iniciador CHAP y de usuario de destino y las contraseñas en la definición de back-end, y hacer que Trident habilite CHAP en la SVM. Con el `useCHAP` Parámetro en la configuración de back-end, Trident autentica las conexiones iSCSI para los back-ends de ONTAP con CHAP. El soporte CHAP bidireccional está disponible con Trident 20.04 y versiones posteriores.

#### Cree y utilice una política de calidad de servicio de SVM

Al aprovechar una política de calidad de servicio de ONTAP, aplicada a la SVM, se limita el número de IOPS consumibles por los volúmenes aprovisionados de Trident. Esto ayuda a. "prevenir un matón" O un contenedor fuera de control que no afecta a las cargas de trabajo fuera de la SVM de Trident.

Puede crear una política de calidad de servicio para la SVM en unos pasos. Consulte la documentación de su versión de ONTAP para obtener la información más precisa. El ejemplo siguiente crea una política de calidad de servicio que limita el total de IOPS disponibles para la SVM a 5000.

```
# create the policy group for the SVM
qos policy-group create -policy-group <policy_name> -vserver <svm_name>
-max-throughput 5000iops

# assign the policy group to the SVM, note this will not work
# if volumes or files in the SVM have existing QoS policies
vserver modify -vserver <svm_name> -qos-policy-group <policy_name>
```

Además, si su versión de ONTAP admite esta función, puede considerar el uso de una calidad de servicio

mínima para garantizar un volumen del rendimiento para cargas de trabajo en contenedores. La calidad de servicio adaptativa no es compatible con una política de nivel de SVM.

El número de IOPS dedicado a las cargas de trabajo de los contenedores depende de muchos aspectos. Entre otras cosas, estas incluyen:

- Otras cargas de trabajo que utilizan la cabina de almacenamiento. Si hay otras cargas de trabajo, no relacionadas con la puesta en marcha de Kubernetes, y que utilizan los recursos de almacenamiento, se debe tener cuidado para garantizar que esas cargas de trabajo no se vean afectadas de forma accidental.
- Cargas de trabajo esperadas que se ejecutan en contenedores. Si las cargas de trabajo que tienen requisitos de IOPS elevados se ejecutan en contenedores, una política de calidad de servicio baja resulta en una mala experiencia.

Es importante recordar que una política de calidad de servicio asignada en el nivel de la SVM da como resultado que todos los volúmenes aprovisionados a la SVM compartan el mismo pool de IOPS. Si una, o una cifra pequeña, de las aplicaciones con contenedores tienen un requisito elevado de IOPS, podría convertirse en un problema para las otras cargas de trabajo con contenedores. Si este es el caso, puede que se desee considerar utilizar la automatización externa para asignar políticas de calidad de servicio por volumen.

> Debe asignar el grupo de políticas QoS al SVM **only** si la versión de ONTAP es anterior a 9.8.

**Cree grupos de políticas de calidad de servicio para Trident**

La calidad de servicio garantiza que el rendimiento de las cargas de trabajo críticas no se vea degradado por cargas de trabajo de la competencia. Los grupos de políticas de calidad de servicio de ONTAP proporcionan opciones de calidad de servicio para volúmenes y permiten a los usuarios definir el techo de rendimiento para una o más cargas de trabajo. Para obtener más información sobre la calidad de servicio, consulte "Rendimiento garantizado con QoS". Puede especificar grupos de políticas de calidad de servicio en el back-end o en un pool de almacenamiento y se aplican a cada volumen creado en ese pool o back-end.

ONTAP tiene dos tipos de grupos de políticas de calidad de servicio: Tradicionales y adaptativos. Los grupos de políticas tradicionales proporcionan un rendimiento máximo (o mínimo, en versiones posteriores) plano en IOPS. La calidad de servicio adaptativa escala automáticamente el rendimiento al tamaño de la carga de trabajo y mantiene la ratio de IOPS en TB|GB a medida que el tamaño de la carga de trabajo cambia. Esto supone una ventaja significativa cuando se gestionan cientos o miles de cargas de trabajo en una puesta en marcha de gran tamaño.

Tenga en cuenta lo siguiente al crear grupos de políticas de calidad de servicio:

- Debe configurar la `qosPolicy` introduzca la `defaults` bloque de la configuración del back-end. Consulte el siguiente ejemplo de configuración del back-end:

```
  ---
version: 1
storageDriverName: ontap-nas
managementLIF: 0.0.0.0
dataLIF: 0.0.0.0
svm: svm0
username: user
password: pass
defaults:
  qosPolicy: standard-pg
storage:
- labels:
    performance: extreme
  defaults:
    adaptiveQosPolicy: extremely-adaptive-pg
- labels:
    performance: premium
  defaults:
    qosPolicy: premium-pg
```

- Debe aplicar los grupos de políticas por volumen, de modo que cada volumen obtenga el rendimiento entero según lo especifique el grupo de políticas. No se admiten los grupos de políticas compartidas.

Para obtener más información sobre los grupos de políticas de calidad de servicio, consulte "Comandos de calidad de servicio de ONTAP 9.8".

#### Limite el acceso a recursos de almacenamiento a los miembros del clúster de Kubernetes

La limitación del acceso a los volúmenes NFS y a las LUN de iSCSI creadas por Trident es un componente crucial del sistema de seguridad para la puesta en marcha de Kubernetes. Si lo hace, se evita que los hosts que no forman parte del clúster de Kubernetes accedan a los volúmenes y que potencialmente modifiquen los datos de forma inesperada.

Es importante comprender que los espacios de nombres son el límite lógico de los recursos en Kubernetes. Se supone que los recursos del mismo espacio de nombres se pueden compartir; sin embargo, es importante destacar que no existe ninguna funcionalidad entre espacios de nombres. Esto significa que aunque los VP sean objetos globales, cuando están enlazados a una RVP solo pueden acceder a ellos mediante POD que están en el mismo espacio de nombres. **Es fundamental asegurarse de que los espacios de nombres se utilizan para proporcionar la separación cuando sea apropiado.**

La preocupación principal de la mayoría de las organizaciones con respecto a la seguridad de los datos en un contexto de Kubernetes es que un proceso en un contenedor puede acceder al almacenamiento montado en el host, pero que no está destinado al contenedor. "Espacios de nombres" están diseñados para evitar este tipo de compromiso. Sin embargo, hay una excepción: Contenedores privilegiados.

Un contenedor con privilegios es uno que se ejecuta con mucho más permisos de nivel de host de lo normal. No se deniegan de forma predeterminada, por lo que debe desactivar la funcionalidad utilizando "directivas de seguridad de pod".

Para los volúmenes en los que se desea obtener acceso tanto a los hosts de Kubernetes como a los externos,

el almacenamiento se debe gestionar de forma tradicional, con el VP introducido por el administrador, y no gestionado por Trident. Esto garantiza que el volumen de almacenamiento se destruya solo cuando tanto los hosts de Kubernetes como los externos se desconectaron y ya no utilizan el volumen. Además, se puede aplicar una política de exportación personalizada, lo que permite el acceso desde los nodos del clúster de Kubernetes y los servidores objetivo fuera del clúster de Kubernetes.

Para las implementaciones que tienen nodos de infraestructura dedicados (por ejemplo, OpenShift) u otros nodos que no pueden programar aplicaciones de usuario, se deben utilizar directivas de exportación independientes para limitar aún más el acceso a los recursos de almacenamiento. Esto incluye la creación de una directiva de exportación para los servicios que se implementan en dichos nodos de infraestructura (por ejemplo, los servicios de registro y métricas de OpenShift) y aplicaciones estándar que se implementan en nodos que no son de infraestructura.

#### Usar una política de exportación dedicada

Debe asegurarse de que existe una política de exportación para cada back-end que solo permita el acceso a los nodos presentes en el clúster de Kubernetes. Trident puede crear y gestionar automáticamente políticas de exportación a partir de la versión 20.04. De esta forma, Trident limita el acceso a los volúmenes que aprovisiona a los nodos en el clúster de Kubernetes y simplifica la adición o la eliminación de nodos.

También puede crear una política de exportación manualmente y rellenarla con una o varias reglas de exportación que procesarán cada solicitud de acceso a nodo:

- Utilice la `vserver export-policy create` Comando de la interfaz de línea de comandos de ONTAP para crear la política de exportación.
- Añada reglas a la política de exportación mediante la `vserver export-policy rule create` Comando de la CLI de ONTAP.

Si ejecuta estos comandos, puede restringir el acceso de los nodos de Kubernetes a los datos.

#### Desactivar `showmount` Para la SVM de la aplicación

La `showmount` Con la función, un cliente NFS puede consultar a la SVM para obtener una lista de exportaciones NFS disponibles. Un pod puesto en marcha en el clúster de Kubernetes puede ejecutar el `showmount -e` Comando en la LIF de datos y recibe una lista de montajes disponibles, incluidos los a los que no tiene acceso. Aunque esto, por sí solo, no supone un compromiso con la seguridad, proporciona información innecesaria, potencialmente que ayuda a un usuario no autorizado a conectarse con una exportación NFS.

Debe desactivar `showmount` Con el comando CLI de ONTAP a nivel de la SVM:

```
vserver nfs modify -vserver <svm_name> -showmount disabled
```

## Mejores prácticas para SolidFire

Conozca las prácticas recomendadas para configurar el almacenamiento de SolidFire para Trident.

#### Crear cuenta de SolidFire

Cada cuenta SolidFire representa un propietario de volumen único y recibe su propio conjunto de credenciales de protocolo de autenticación por desafío mutuo (CHAP). Es posible acceder a los volúmenes asignados a una cuenta mediante el nombre de cuenta y las credenciales CHAP relativas o un grupo de acceso de

volúmenes. Una cuenta puede tener hasta 2000 volúmenes asignados, pero un volumen solo puede pertenecer a una cuenta.

### Cree una política de calidad de servicio

Utilice las políticas de calidad de servicio de SolidFire si desea crear y guardar un ajuste de calidad de servicio estandarizado que se puede aplicar a muchos volúmenes.

Puede establecer parámetros de calidad de servicio por cada volumen. El rendimiento de cada volumen se puede garantizar mediante el establecimiento de tres parámetros configurables que definen la calidad de servicio: Min IOPS, Max IOPS y Burst IOPS.

Aquí pueden ver los valores mínimos, máximos y de ráfaga de IOPS en relación con el tamaño de bloque de 4 KB.

| Parámetro IOPS | Definición | Espacio valor | Valor predeterminado | Capacidad Valor (4 KB) |
|---|---|---|---|---|
| IOPS mín | El nivel garantizado de rendimiento de un volumen. | 50 | 50 | 15000 |
| Tasa máx. De IOPS | El rendimiento no superará este límite. | 50 | 15000 | 200,000 |
| IOPS de ráfaga | IOPS máximo permitido en un escenario de ráfaga breve. | 50 | 15000 | 200,000 |

> Aunque Max IOPS y Burst IOPS se pueden establecer con un valor máximo de 200,000 000, el rendimiento máximo en el mundo real de un volumen se ve limitado por el uso del clúster y el rendimiento por cada nodo.

El tamaño de bloque y el ancho de banda influyen directamente en el número de IOPS. A medida que estos aumenten, el sistema aumentará el ancho de banda hasta el nivel que necesite para procesar los tamaños de bloque más grandes. A medida que aumenta el ancho de banda, se reduce el número de IOPS que el sistema es capaz de conseguir. Consulte "Calidad de servicio de SolidFire" Para obtener más información sobre la calidad de servicio y el rendimiento.

### Autenticación SolidFire

Element admite dos métodos para la autenticación: CHAP y grupos de acceso de volumen (VAG). CHAP utiliza el protocolo CHAP para autenticar el host al back-end. Los grupos de acceso de volúmenes controlan el acceso a los volúmenes que aprovisiona. NetApp recomienda utilizar CHAP para la autenticación, ya que es más sencillo y sin límites de escalado.

> Trident con el aprovisionador CSI mejorado admite el uso de la autenticación CHAP. Los VAG sólo deben utilizarse en el modo de funcionamiento tradicional no CSI.

La autenticación CHAP (verificación de que el iniciador es el usuario de volumen objetivo) solo se admite con control de acceso basado en la cuenta. Si se utiliza CHAP para la autenticación, hay dos opciones

disponibles: CHAP unidireccional y CHAP bidireccional. CHAP unidireccional autentica el acceso al volumen mediante el nombre de cuenta de SolidFire y el secreto de iniciador. La opción CHAP bidireccional proporciona la manera más segura de autenticar el volumen, ya que el volumen autentica el host a través del nombre de cuenta y el secreto de iniciador, y luego el host autentica el volumen por medio del nombre de cuenta y el secreto de destino.

Sin embargo, si no se puede habilitar CHAP y se requieren los VAG, cree el grupo de acceso y añada los iniciadores de host y los volúmenes al grupo de acceso. Cada IQN que se añade a un grupo de acceso puede acceder a cada volumen del grupo con o sin autenticación CHAP. Si el iniciador de iSCSI está configurado para utilizar la autenticación CHAP, se utiliza el control de acceso basado en cuentas. Si el iniciador iSCSI no está configurado para utilizar la autenticación CHAP, se utiliza el control de acceso del grupo de acceso de volúmenes.

### ¿Dónde encontrar más información?

A continuación se enumeran algunas de las prácticas recomendadas. Busque en el "Biblioteca de NetApp" para las versiones más actuales.

**ONTAP**

- "Prácticas recomendadas y guía de implementación de NFS"
- "Guía de administración de SAN" (Para iSCSI)
- "Configuración exprés de iSCSI para RHEL"

**Software Element**

- "Configuración de SolidFire para Linux"

**NetApp HCI**

- "Requisitos previos de la implementación de NetApp HCI"
- "Acceda al motor de implementación de NetApp"

**Información sobre las prácticas recomendadas de la aplicación**

- "Prácticas recomendadas para MySQL en ONTAP"
- "Prácticas recomendadas para MySQL en SolidFire"
- "NetApp SolidFire y Cassandra"
- "Prácticas recomendadas de Oracle en SolidFire"
- "Prácticas recomendadas de PostgreSQL en SolidFire"

No todas las aplicaciones tienen directrices específicas, es importante trabajar con su equipo de NetApp y utilizar el "Biblioteca de NetApp" para encontrar la documentación más actualizada.

# Integre Astra Trident

Para integrar Astra Trident, los siguientes elementos de diseño y arquitectura requieren integración: Selección y puesta en marcha de controladores, diseño de clase de almacenamiento, diseño de pools virtuales, efecto de la reclamación de volumen persistente (PVC) en el aprovisionamiento de almacenamiento, las operaciones de

volumen y la puesta en marcha de servicios OpenShift con Astra Trident.

## Selección y despliegue del conductor

Seleccione e implemente un controlador de back-end para el sistema de almacenamiento.

### Controladores de entorno de administración ONTAP

Los controladores de entorno de administración de ONTAP se diferencian por el protocolo utilizado y cómo se aprovisionan los volúmenes en el sistema de almacenamiento. Por lo tanto, tenga cuidado al decidir qué controlador implementar.

En un nivel superior, si la aplicación cuenta con componentes que necesitan almacenamiento compartido (varios POD que acceden al mismo PVC), los controladores basados en NAS serán la opción predeterminada, mientras que los controladores iSCSI basados en bloques satisfacen las necesidades de almacenamiento no compartido. Elija el protocolo según los requisitos de la aplicación y el nivel de comodidad de los equipos de almacenamiento e infraestructura. Por lo general, existe poca diferencia entre ellas para la mayoría de las aplicaciones, con tanta frecuencia la decisión se basa en si se necesita o no almacenamiento compartido (donde más de un pod necesitará acceso simultáneo).

Los controladores de entorno de administración de ONTAP disponibles son:

- `ontap-nas`: Cada PV aprovisionado es un FlexVolume ONTAP completo.
- `ontap-nas-economy`: Cada PV aprovisionado es un qtree, con un número configurable de qtrees por FlexVolume (el valor predeterminado es 200).
- `ontap-nas-flexgroup`: Cada VP aprovisionado como ONTAP FlexGroup completo y se utilizan todos los agregados asignados a una SVM.
- `ontap-san`: Cada PV aprovisionado es una LUN dentro de su propio FlexVolume.
- `ontap-san-economy`: Cada VP aprovisionado es una LUN, con un número configurable de LUN por FlexVolume (el valor predeterminado es 100).

La elección entre los tres controladores NAS tiene algunas ramificaciones a las funciones, que están disponibles para la aplicación.

Tenga en cuenta que, en las siguientes tablas, no todas las funcionalidades se exponen a través de Astra Trident. El administrador de almacenamiento debe aplicar algunas después del aprovisionamiento si se desea disponer de esta funcionalidad. Las notas al pie de la superíndice distinguen la funcionalidad por característica y controlador.

| Unidades NAS de ONTAP | Snapshot | Clones | Políticas de exportación dinámicas | Conexión múltiple | Calidad de servicio | Cambie el tamaño | Replicación |
|---|---|---|---|---|---|---|---|
| `ontap-nas` | Sí | Sí | Yespie de página:5[] | Sí | Yespie de página:1[] | Sí | Yespie de página:1[] |
| `ontap-nas-economy` | Yespie de página:3[] | Yespie de página:3[] | Yespie de página:5[] | Sí | Yespie de página:3[] | Sí | Yespie de página:3[] |
| `ontap-nas-flexgroup` | Yespie de página:1[] | No | Yespie de página:5[] | Sí | Yespie de página:1[] | Sí | Yespie de página:1[] |

Astra Trident ofrece 2 controladores SAN para ONTAP, cuyas funciones se muestran a continuación.

| Unidades SAN de ONTAP | Snapshot | Clones | Conexión múltiple | CHAP bidireccional | Calidad de servicio | Cambie el tamaño | Replicación |
|---|---|---|---|---|---|---|---|
| `ontap-san` | Sí | Sí | Yespie de página:4[] | Sí | Yespie de página:1[] | Sí | Yespie de página:1[] |
| `ontap-san-economy` | Sí | Sí | Yespie de página:4[] | Sí | Yespie de página:3[] | Sí | Yespie de página:3[] |

> Nota al pie de página para las tablas anteriores: Yesnota al pie:1[]: No administrado por Astra Trident Yesnota al pie de página:2[]: Administrado por Astra Trident, pero no por PV Yesnota 3 al pie de página granular:4[]: Compatible con volúmenes de bloque bruto Yesnota al pie de página:5[]: Respaldado por CSI Trident

Las funciones que no son granulares en los VP se aplican a todo el FlexVolume y todos los VP (es decir, qtrees o LUN de FlexVols compartidos) compartirán un programa común.

Como podemos ver en las tablas anteriores, gran parte de la funcionalidad entre `ontap-nas` y.. `ontap-nas-economy` es lo mismo. Sin embargo, porque la `ontap-nas-economy` Esta unidad limita la capacidad de controlar la programación con una granularidad VP, lo que puede afectar a su planificación de backup y recuperación ante desastres en concreto. En el caso de los equipos de desarrollo que desean aprovechar la funcionalidad de clonado de PVC en el almacenamiento de ONTAP, esto solo es posible cuando se utiliza la `ontap-nas`, `ontap-san` o. `ontap-san-economy` de windows

> La `solidfire-san` El controlador también es capaz de clonar EVs.

#### Controladores de entorno de administración Cloud Volumes ONTAP

Cloud Volumes ONTAP proporciona control de datos junto con funciones de almacenamiento empresarial para diversos casos de uso, como recursos compartidos de archivos y almacenamiento a nivel de bloque que presta servicio a protocolos NAS y SAN (NFS, SMB/CIFS e iSCSI). Los controladores compatibles para Cloud Volume ONTAP son `ontap-nas`, `ontap-nas-economy`, `ontap-san` y.. `ontap-san-economy`. Estos son aplicables a Cloud Volume ONTAP para Azure, Cloud Volume ONTAP para GCP.

#### Controladores de entorno de administración de Amazon FSX para ONTAP

Amazon FSX para ONTAP permite a los clientes aprovechar las funciones, el rendimiento y las funcionalidades administrativas de NetApp con las que ya están familiarizados, a la vez que aprovechan la simplicidad, la agilidad, la seguridad y la escalabilidad de almacenar datos en AWS. FSX para ONTAP es compatible con muchas de las API de administración y las funciones del sistema de archivos de ONTAP. Los controladores compatibles para Cloud Volume ONTAP son `ontap-nas`, `ontap-nas-economy`, `ontap-nas-flexgroup`, `ontap-san` y.. `ontap-san-economy`.

#### Controladores de back-end de HCI/SolidFire de NetApp

La `solidfire-san` El controlador que se utiliza con las plataformas HCI/SolidFire de NetApp, ayuda al administrador a configurar un back-end de Element para Trident según los límites de calidad de servicio. Si desea diseñar el back-end de modo que establezca los límites de calidad de servicio específicos en los volúmenes aprovisionados por Trident, utilice la `type` parámetro en el archivo back-end. El administrador

también puede restringir el tamaño del volumen que podría crearse en el almacenamiento mediante el `limitVolumeSize` parámetro. Actualmente, las funciones de almacenamiento de Element, como el cambio de tamaño de volumen y la replicación de volumen, no se admiten mediante el `solidfire-san` controlador. Estas operaciones se deben realizar manualmente mediante la interfaz de usuario web del software Element.

| Controlador SolidFire | Snapshot | Clones | Conexión múltiple | CHAP | Calidad de servicio | Cambie el tamaño | Replicación |
|---|---|---|---|---|---|---|---|
| `solidfire-san` | Sí | Sí | Yespie de página:2[] | Sí | Sí | Sí | Yespie de página:1[] |

> Nota al pie: Yesfonote:1[]: No administrado por Astra Trident Yes [2]: Admitido para volúmenes de bloque RAW

#### Controladores de entorno de administración Azure NetApp Files

Astra Trident utiliza `azure-netapp-files` controlador para administrar "Azure NetApp Files" servicio.

Puede encontrar más información acerca de este controlador y cómo configurarlo en "Configuración de back-end de Astra Trident para Azure NetApp Files".

| Controlador Azure NetApp Files | Snapshot | Clones | Conexión múltiple | Calidad de servicio | Expanda | Replicación |
|---|---|---|---|---|---|---|
| `azure-netapp-files` | Sí | Sí | Sí | Sí | Sí | Yespie de página:1[] |

> Pie de página: Yesfonote:1[]: No administrado por Astra Trident

#### Cloud Volumes Service en el controlador back-end de Google Cloud

Astra Trident utiliza `gcp-cvs` Controlador para vincular con Cloud Volumes Service en Google Cloud.

La `gcp-cvs` La unidad utiliza pools virtuales para abstraer el back-end y permitir a Astra Trident determinar la ubicación del volumen. El administrador define los pools virtuales en `backend.json` archivos. Las clases de almacenamiento utilizan selectores para identificar los pools virtuales por etiqueta.

- Si se definen pools virtuales en el back-end, Astra Trident intentará crear un volumen en los pools de almacenamiento de Google Cloud a los que están limitados esos pools virtuales.
- Si no se definen pools virtuales en el back-end, Astra Trident selecciona un pool de almacenamiento de Google Cloud de los pools de almacenamiento disponibles en la región.

Para configurar el back-end de Google Cloud en Astra Trident, debe especificar `projectNumber`, `apiRegion`, y. `apiKey` en el archivo de fondo. Puede encontrar el número de proyecto en la consola de Google Cloud. La clave API se obtiene del archivo de claves privadas de la cuenta de servicio que creó al configurar el acceso de API para Cloud Volumes Service en Google Cloud.

Para obtener más información sobre Cloud Volumes Service en los tipos de servicio y niveles de servicio de Google Cloud, consulte "Obtenga más información sobre la compatibilidad de Astra Trident con CVS para GCP".

| Controlador de Cloud Volumes Service para Google Cloud | Snapshot | Clones | Conexión múltiple | Calidad de servicio | Expanda | Replicación |
|---|---|---|---|---|---|---|
| `gcp-cvs` | Sí | Sí | Sí | Sí | Sí | Disponible solo en el tipo de servicio CVS-Performance. |

**Notas de replicación**

- Astra Trident no gestiona la replicación.
- El clon se creará en el mismo pool de almacenamiento que el volumen de origen.

## Diseño de clase de almacenamiento

Las clases de almacenamiento individuales deben configurarse y aplicarse para crear un objeto de clase de almacenamiento Kubernetes. En esta sección se analiza cómo diseñar una clase de almacenamiento para su aplicación.

### Utilización de back-end específica

El filtrado se puede usar en un objeto de clase de almacenamiento específico para determinar el pool o conjunto de pools de almacenamiento que se utilizarán con esa clase de almacenamiento específica. Se pueden establecer tres conjuntos de filtros en la clase de almacenamiento: `storagePools`, `additionalStoragePools`, y/o. `excludeStoragePools`.

La `storagePools` el parámetro ayuda a restringir el almacenamiento al conjunto de pools que coinciden con cualquier atributo especificado. La `additionalStoragePools` El parámetro se utiliza para ampliar el conjunto de pools que utilizará Astra Trident para el aprovisionamiento junto con el conjunto de pools seleccionados por los atributos y. `storagePools` parámetros. Es posible usar un parámetro de forma independiente o ambos juntos para garantizar que se seleccione el conjunto adecuado de pools de almacenamiento.

La `excludeStoragePools` el parámetro se utiliza para excluir específicamente el conjunto de pools enumerado que coincide con los atributos.

### Emular las políticas de calidad de servicio

Si desea diseñar clases de almacenamiento para emular políticas de calidad de servicio, cree una clase de almacenamiento con la `media` atributo como `hdd` o. `ssd`. Según la `media` Atributo mencionado en la clase de almacenamiento, Trident seleccionará el back-end apropiado `hdd` o. `ssd` agregados para coincidir con el atributo de medios y, a continuación, dirigir el aprovisionamiento de los volúmenes al agregado específico. Por tanto, podemos crear UNA CLASE PREMIUM DE almacenamiento que tendría `media` atributo establecido como `ssd` Las cuales pueden clasificarse como política DE calidad DE servicio PREMIUM. Podemos crear otro ESTÁNDAR de clase de almacenamiento que tenga el conjunto de atributos de medios como "hdd", que podría clasificarse como política DE calidad DE servicio ESTÁNDAR. También podríamos usar el atributo "IOPS" en la clase de almacenamiento para redirigir el aprovisionamiento a un dispositivo Element que se puede definir como una Política de calidad de servicio.

### Utilizar back-end basado en funciones específicas

Las clases de almacenamiento se pueden diseñar para dirigir el aprovisionamiento de volúmenes en un entorno de administración específico, donde se habilitan funciones como thin provisioning y thick, copias Snapshot, clones y cifrado. Para especificar qué almacenamiento se debe utilizar, cree clases de almacenamiento que especifiquen el back-end adecuado con la función necesaria habilitada.

### Pools virtuales

Hay pools virtuales disponibles para todos los back-ends de Astra Trident. Puede definir pools virtuales para cualquier back-end a través de cualquier controlador que proporcione Astra Trident.

Los pools virtuales permiten a un administrador crear un nivel de abstracción sobre los back-ends que se puede hacer referencia a través de las clases de almacenamiento, para obtener mayor flexibilidad y colocación eficiente de los volúmenes en back-ends. Pueden definirse distintos back-ends con la misma clase de servicio. Es más, es posible crear varios pools de almacenamiento en el mismo back-end, pero con características diferentes. Cuando se configura una clase de almacenamiento con un selector con las etiquetas específicas, Astra Trident elige un back-end que coincide con todas las etiquetas de selector para colocar el volumen. Si las etiquetas del selector de clase de almacenamiento coinciden con varios pools de almacenamiento, Astra Trident elegirá una de ellas para aprovisionar el volumen desde.

## Diseño de pool virtual

Al crear un back-end, generalmente puede especificar un conjunto de parámetros. Era imposible que el administrador creara otro back-end con las mismas credenciales de almacenamiento y con un conjunto de parámetros diferente. Con la introducción de pools virtuales, este problema se ha aliviado. Los pools virtuales son una abstracción de niveles introducida entre el back-end y la clase de almacenamiento de Kubernetes de modo que el administrador puede definir parámetros junto con etiquetas a las que se puede hacer referencia a través de las clases de almacenamiento de Kubernetes como selector, de forma independiente del back-end. Es posible definir pools virtuales para todos los back-ends de NetApp compatibles con Astra Trident. Esta lista incluye HCI de SolidFire/NetApp, ONTAP, Cloud Volumes Service en GCP y Azure NetApp Files.

> Al definir los pools virtuales, se recomienda no intentar reorganizar el orden de los grupos virtuales existentes en una definición de backend. También es aconsejable no editar/modificar atributos para un pool virtual existente y definir un nuevo pool virtual en su lugar.

### Emulación de distintos niveles de servicio/calidad de servicio

Se pueden diseñar pools virtuales para emular clases de servicio. Al utilizar la implementación de pools virtuales para el servicio Cloud Volume para Azure NetApp Files, examinemos cómo podemos configurar distintas clases de servicio. Configure el backend ANF con varias etiquetas, que representan diferentes niveles de rendimiento. Configurado `servicelevel` aspecto al nivel de rendimiento apropiado y agregar otros aspectos requeridos en cada etiqueta. Ahora cree diferentes clases de almacenamiento de Kubernetes que se asignarán a diferentes pools virtuales. Con el `parameters.selector` Campo, cada clase de almacenamiento llama a qué pools virtuales se pueden utilizar para alojar un volumen.

### Asignación de un conjunto específico de aspectos

Se pueden diseñar varios pools virtuales con un conjunto específico de aspectos a partir de un único back-end de almacenamiento. Para ello, configure el backend con varias etiquetas y defina los aspectos necesarios en cada etiqueta. Ahora cree diferentes clases de almacenamiento de Kubernetes usando `parameters.selector` campo que se asignará a diferentes pools virtuales. Los volúmenes que se aprovisionan en el back-end tendrán los aspectos definidos en el pool virtual elegido.

### Las características de PVC que afectan al aprovisionamiento de almacenamiento

Algunos parámetros que superen la clase de almacenamiento solicitada pueden afectar al proceso de decisión de aprovisionamiento de Astra Trident al crear una RVP.

#### Modo de acceso

Al solicitar un almacenamiento a través de un PVC, uno de los campos obligatorios es el modo de acceso. El modo deseado puede afectar el back-end seleccionado para alojar la solicitud de almacenamiento.

Astra Trident intentará igualar el protocolo de almacenamiento que se utiliza con el método de acceso especificado según la siguiente matriz. Es independiente de la plataforma de almacenamiento subyacente.

| | ReadWriteOnce | ReadOnlyMany | ReadWriteMany |
|---|---|---|---|
| ISCSI | Sí | Sí | Sí (bloque sin formato) |
| NFS | Sí | Sí | Sí |

Si se solicita un PVC ReadWriteMany enviado a una implementación de Trident sin un back-end de NFS configurado, no se aprovisionará ningún volumen. Por este motivo, el solicitante debe usar el modo de acceso adecuado para su aplicación.

## Operaciones de volumen

### Modifique los volúmenes persistentes

Los volúmenes persistentes son, con dos excepciones, objetos inmutables en Kubernetes. Una vez creada, la política de reclamaciones y el tamaño se pueden modificar. Sin embargo, esto no impide que se modifiquen algunos aspectos del volumen fuera de Kubernetes. Esto puede ser deseable para personalizar el volumen para aplicaciones específicas, con el fin de garantizar que la capacidad no se consume accidentalmente, o simplemente mover el volumen a una controladora de almacenamiento diferente por cualquier motivo.

> Los aprovisionadores de árbol de Kubernetes no admiten las operaciones de cambio de tamaño de volumen para NFS o iSCSI VP en este momento. Astra Trident admite la ampliación de volúmenes NFS e iSCSI.

Los detalles de conexión del VP no se pueden modificar una vez creado.

### Cree snapshots de volumen bajo demanda

Astra Trident admite la creación de instantáneas de volumen bajo demanda y la creación de EVs a partir de instantáneas utilizando el marco CSI. Las copias Snapshot proporcionan un método cómodo de mantener copias de un momento específico de los datos y poseen un ciclo de vida independiente del VP de origen de Kubernetes. Estas instantáneas se pueden utilizar para clonar EVs.

### Crear volúmenes a partir de snapshots

Astra Trident también admite la creación de volúmenes PersistentVolumes a partir de snapshots de volúmenes. Para ello, sólo tiene que crear una reclamación de volumen persistente y mencionar la `datasource` como la snapshot necesaria a partir de la que se debe crear el volumen. Astra Trident se encargará de gestionar esta RVP mediante la creación de un volumen con los datos presentes en la snapshot. Con esta función, es posible duplicar datos entre regiones, crear entornos de prueba, reemplazar un volumen de producción dañado o dañado en su totalidad, o recuperar archivos y directorios específicos y transferirlos a

otro volumen adjunto.

### Mueva volúmenes al clúster

Los administradores de almacenamiento pueden mover volúmenes entre agregados y controladoras en el clúster de ONTAP de forma no disruptiva al consumidor de almacenamiento. Esta operación no afecta al clúster Astra Trident o Kubernetes, siempre y cuando el agregado de destino sea el que utilice la SVM a la que Astra Trident tenga acceso. Lo que es importante: Si el agregado se ha añadido recientemente a la SVM, deberá actualizar el back-end añadiendo de nuevo a Astra Trident. Esto hará que Astra Trident vuelva a realizar el inventario de las SVM para que se reconozca el nuevo agregado.

Sin embargo, Astra Trident no admite automáticamente la transferencia de volúmenes entre back-ends. Esto incluye entre SVM en el mismo clúster, entre clústeres o en una plataforma de almacenamiento diferente (incluso si ese sistema de almacenamiento está conectado a Astra Trident).

Si se copia un volumen en otra ubicación, es posible utilizar la función de importación de volúmenes para importar los volúmenes actuales a Astra Trident.

### Expanda los volúmenes

Astra Trident admite el cambio de tamaño de VP iSCSI y NFS. De este modo, los usuarios pueden cambiar el tamaño de sus volúmenes directamente desde la capa de Kubernetes. La expansión de volumen es posible para las principales plataformas de almacenamiento de NetApp, como ONTAP, HCI de SolidFire/NetApp y back-ends de Cloud Volumes Service. Para permitir una posible expansión más adelante, establezca `allowVolumeExpansion` para `true` En el tipo de almacenamiento asociado con el volumen. Siempre que sea necesario cambiar el tamaño del volumen persistente, edite el `spec.resources.requests.storage` Anotación en la reclamación de volumen persistente al tamaño de volumen requerido. Trident se ocupa automáticamente de ajustar el tamaño del volumen en el clúster de almacenamiento.

### Importe un volumen existente en Kubernetes

La importación de volúmenes ofrece la posibilidad de importar un volumen de almacenamiento existente en un entorno de Kubernetes. Actualmente es compatible con `ontap-nas`, `ontap-nas-flexgroup`, `solidfire-san`, `azure-netapp-files`, y. `gcp-cvs` de windows Esta función es útil cuando se pasa una aplicación existente a Kubernetes o durante escenarios de recuperación ante desastres.

Cuando utilice las ONTAP y. `solidfire-san` controladores, utilice el comando `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` Para importar un volumen existente a Kubernetes y que Astra Trident gestione. El archivo PVC YLMA o JSON que se usa en el comando import volume señala a una clase de almacenamiento que identifica a Astra Trident como el aprovisionador. Cuando se utiliza un back-end de HCI/SolidFire de NetApp, asegúrese de que los nombres de los volúmenes sean únicos. Si los nombres de los volúmenes se duplican, clone el volumen en un nombre único de modo que la función de importación de volumen pueda distinguir entre ellos.

Si la `azure-netapp-files` o. `gcp-cvs` se utiliza el controlador, utilice el comando `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml` Para importar el volumen a Kubernetes que gestiona Astra Trident. Esto garantiza una referencia de volumen única.

Una vez ejecutado el comando anterior, Astra Trident encontrará el volumen en el back-end y leerá su tamaño. Agregará automáticamente (y sobrescribirá si es necesario) el tamaño del volumen del PVC configurado. A continuación, Astra Trident crea el nuevo VP y Kubernetes enlaza la RVP con el VP.

Si se puso en marcha un contenedor de modo que requería la RVP específica importada, este permanecería en estado pendiente hasta que el par PVC/VP se enlaza a través del proceso de importación del volumen. Una vez enlazados el par PVC/PV, el contenedor debería aparecer, siempre que no haya otros problemas.

## Implementar servicios OpenShift

Los servicios de clúster de valor añadido de OpenShift proporcionan una funcionalidad importante a los administradores de clúster y a las aplicaciones que se alojan. Sin embargo, el almacenamiento que utilizan estos servicios puede aprovisionarse con los recursos locales de nodos, esto limita con frecuencia la capacidad, el rendimiento, la capacidad de recuperación y la sostenibilidad del servicio. Sin embargo, al aprovechar una cabina de almacenamiento empresarial para ofrecer la capacidad de estos servicios se puede mejorar considerablemente el servicio. Al igual que sucede con todas las aplicaciones, OpenShift y los administradores de almacenamiento deberían trabajar estrechamente para determinar cuáles son las mejores opciones para cada uno de ellos. La documentación de Red Hat debe utilizarse en gran medida para determinar los requisitos y garantizar que se satisfagan las necesidades de tamaño y rendimiento.

### Servicio de registro

Se ha documentado en la implementación y administración del almacenamiento para el registro "netapp.io" en la "blog".

### Servicio de registro

Al igual que otros servicios OpenShift, el servicio de registro se pone en marcha con Ansible, con parámetros de configuración suministrados por el archivo de inventario, también conocido como los hosts, que se proporcionan al libro de estrategia. Hay dos métodos de instalación que se tratarán: Implementar el registro durante la instalación inicial de OpenShift y desplegar el registro después de que OpenShift haya sido instalado.

> A partir de Red Hat OpenShift versión 3.9, la documentación oficial recomienda contra NFS para el servicio de registro debido a problemas relacionados con la corrupción de datos. Esto se basa en las pruebas de Red Hat de sus productos. El servidor NFS de ONTAP no tiene estos problemas y puede realizar fácilmente una implementación de registro. Finalmente, la elección del protocolo para el servicio de registro depende de usted; simplemente sabe que ambos funcionarán bien cuando usen las plataformas de NetApp y no hay motivos para evitar NFS si eso es lo que prefiere.

Si decide utilizar NFS con el servicio de registro, tendrá que establecer la variable Ansible `openshift_enable_unsupported_configurations` para `true` para evitar que el instalador falle.

#### Manos a la obra

Opcionalmente, el servicio de registro puede implementarse tanto para aplicaciones como para las operaciones principales del propio clúster OpenShift. Si decide implementar el registro de operaciones, especificando la variable `openshift_logging_use_ops` como `true`, se crearán dos instancias del servicio. Las variables que controlan la instancia de registro de las operaciones contienen "OPS" en ellas, mientras que la instancia de las aplicaciones no.

Es importante configurar las variables de Ansible según el método de puesta en marcha para garantizar que los servicios subyacentes utilizan el almacenamiento correcto. Veamos las opciones de cada uno de los métodos de implementación.

> Las siguientes tablas sólo contienen las variables que son relevantes para la configuración de almacenamiento, ya que están relacionadas con el servicio de registro. Puede encontrar otras opciones en "Documentación de registro de RedHat OpenShift" que deben revisarse, configurarse y utilizarse en función de la puesta en marcha.

Las variables de la siguiente tabla harán que el libro de estrategia de Ansible cree un VP y una RVP para el servicio de registro con los detalles proporcionados. Este método es significativamente menos flexible que usar la tableta playbook de instalación de componentes después de la instalación de OpenShift; sin embargo, si tiene volúmenes existentes disponibles, es una opción.

| Variable | Detalles |
|---|---|
| `openshift_logging_storage_kind` | Establezca en `nfs` Para que el instalador cree un PV de NFS para el servicio de registro. |
| `openshift_logging_storage_host` | El nombre de host o la dirección IP del host NFS. Esto debe configurarse en la LIF de datos de su máquina virtual. |
| `openshift_logging_storage_nfs_directory` | La ruta de montaje para la exportación NFS. Por ejemplo, si el volumen se juntan como `/openshift_logging`, utilizaría esa ruta de acceso para esta variable. |
| `openshift_logging_storage_volume_name` | El nombre, por ejemplo `pv_ose_logs`, Del PV que se va a crear. |
| `openshift_logging_storage_volume_size` | Por ejemplo, el tamaño de la exportación NFS `100Gi`. |

Si su clúster OpenShift ya se está ejecutando y, por lo tanto, Trident se ha implementado y configurado, el instalador puede utilizar el aprovisionamiento dinámico para crear los volúmenes. Será necesario configurar las siguientes variables.

| Variable | Detalles |
|---|---|
| `openshift_logging_es_pvc_dynamic` | Establezca esta opción en true para usar volúmenes aprovisionados dinámicamente. |
| `openshift_logging_es_pvc_storage_class_name` | El nombre de la clase de almacenamiento que se utilizará en la RVP. |
| `openshift_logging_es_pvc_size` | El tamaño del volumen solicitado en la RVP. |
| `openshift_logging_es_pvc_prefix` | Prefijo para los EVs que utiliza el servicio de registro. |
| `openshift_logging_es_ops_pvc_dynamic` | Establezca en `true` para utilizar volúmenes aprovisionados de forma dinámica para la instancia de registro de operaciones. |
| `openshift_logging_es_ops_pvc_storage_class_name` | Nombre de la clase de almacenamiento para la instancia de registro de operaciones. |
| `openshift_logging_es_ops_pvc_size` | El tamaño de la solicitud de volumen para la instancia de operaciones. |
| `openshift_logging_es_ops_pvc_prefix` | Prefijo para las RVP de instancia de OPS. |

#### Despliegue la pila de registro

Si va a implementar el registro como parte del proceso de instalación inicial de OpenShift, sólo tendrá que seguir el proceso de implementación estándar. Ansible configurará y pondrá en marcha los servicios y los objetos de OpenShift necesarios para que el servicio esté disponible tan pronto como finalice Ansible.

No obstante, si se pone en marcha después de la instalación inicial, Ansible deberá usar el libro de estrategia

de los componentes. Este proceso puede cambiar ligeramente con diferentes versiones de OpenShift, así que asegúrese de leer y seguir "Documentación de Red Hat OpenShift Container Platform 3.11" para su versión.

## Servicio de métricas

El servicio de métricas proporciona al administrador información valiosa sobre el estado, la utilización de recursos y la disponibilidad del clúster OpenShift. También es necesaria para la funcionalidad de escala automática en pod y muchas organizaciones usan datos del servicio de mediciones para su cargo y/o para mostrar aplicaciones.

Al igual que sucede con el servicio de registro y OpenShift en su conjunto, Ansible se utiliza para poner en marcha el servicio de métricas. Además, al igual que el servicio de registro, el servicio de mediciones se puede implementar durante una configuración inicial del clúster o después de su funcionamiento mediante el método de instalación de componentes. Las siguientes tablas contienen las variables importantes a la hora de configurar el almacenamiento persistente para el servicio de métricas.

> Las siguientes tablas solo contienen las variables relevantes para la configuración del almacenamiento en cuanto se relaciona con el servicio de mediciones. Hay muchas otras opciones en la documentación que se deben revisar, configurar y utilizar de acuerdo con su implementación.

| Variable | Detalles |
|---|---|
| `openshift_metrics_storage_kind` | Establezca en `nfs` Para que el instalador cree un PV de NFS para el servicio de registro. |
| `openshift_metrics_storage_host` | El nombre de host o la dirección IP del host NFS. Esto debe configurarse en el LIF de datos de su SVM. |
| `openshift_metrics_storage_nfs_directory` | La ruta de montaje para la exportación NFS. Por ejemplo, si el volumen se juntan como `/openshift_metrics`, utilizaría esa ruta de acceso para esta variable. |
| `openshift_metrics_storage_volume_name` | El nombre, por ejemplo `pv_ose_metrics`, Del PV que se va a crear. |
| `openshift_metrics_storage_volume_size` | Por ejemplo, el tamaño de la exportación NFS `100Gi`. |

Si su clúster OpenShift ya se está ejecutando y, por lo tanto, Trident se ha implementado y configurado, el instalador puede utilizar el aprovisionamiento dinámico para crear los volúmenes. Será necesario configurar las siguientes variables.

| Variable | Detalles |
|---|---|
| `openshift_metrics_cassandra_pvc_prefix` | Prefijo que se utiliza para las RVP de métricas. |
| `openshift_metrics_cassandra_pvc_size` | El tamaño de los volúmenes que se van a solicitar. |
| `openshift_metrics_cassandra_storage_type` | El tipo de almacenamiento que se utilizará para las métricas, debe establecerse una dinámica para que Ansible cree RVP con la clase de almacenamiento adecuada. |
| `openshift_metrics_cassanda_pvc_storage_class_name` | El nombre de la clase de almacenamiento que se va a utilizar. |

#### Implementar el servicio de métricas

Con las variables de Ansible definidas en el archivo de hosts/inventario, ponga en marcha el servicio con Ansible. Si va a implementar en el momento de la instalación de OpenShift, el PV se creará y utilizará automáticamente. Si pone en marcha usando los libros de estrategia de los componentes, después de la instalación de OpenShift, Ansible creará las RVP necesarias y, una vez que Astra Trident ha aprovisionado el almacenamiento para ellos, pondrá en marcha el servicio.

Las variables anteriores y el proceso de implementación pueden cambiar con cada versión de OpenShift. Asegúrese de revisar y seguir "Guía de implementación de OpenShift de redhat" para su versión de modo que esté configurada para su entorno.

# Protección de datos

Conozca las opciones de protección de datos y capacidad de recuperación que ofrecen las plataformas de almacenamiento de NetApp. Astra Trident puede aprovisionar volúmenes que puedan aprovechar algunas de estas funciones. Debería tener una estrategia de protección y recuperación de datos para cada aplicación con un requisito de persistencia.

## Realice una copia de seguridad del `etcd` datos del clúster

Astra Trident almacena sus metadatos en el clúster de Kubernetes `etcd` base de datos. Realizar una copia de seguridad periódica del `etcd` Los datos del clúster son importantes para recuperar los clústeres de Kubernetes en situaciones de desastre.

#### Pasos

1. La `etcdctl snapshot save` comando permite realizar una copia snapshot de un momento específico de `etcd` clúster:

   ```
   sudo docker run --rm -v /backup:/backup \
     --network host \
     -v /etc/kubernetes/pki/etcd:/etc/kubernetes/pki/etcd \
     --env ETCDCTL_API=3 \
     registry.k8s.io/etcd-amd64:3.2.18 \
     etcdctl --endpoints=https://127.0.0.1:2379 \
     --cacert=/etc/kubernetes/pki/etcd/ca.crt \
     --cert=/etc/kubernetes/pki/etcd/healthcheck-client.crt \
     --key=/etc/kubernetes/pki/etcd/healthcheck-client.key \
     snapshot save /backup/etcd-snapshot.db
   ```

   Este comando crea una instantánea etcd girando un contenedor etcd y lo guarda en `/backup` directorio.

2. En caso de desastre, puede iniciar un clúster de Kubernetes usando las snapshots de etcd. Utilice la `etcdctl snapshot restore` comando para restaurar una instantánea específica realizada en la `/var/lib/etcd` carpeta. Después de la restauración, confirme si `/var/lib/etcd` se ha completado la carpeta con `member` carpeta. A continuación se muestra un ejemplo de `etcdctl snapshot restore` comando:

```
etcdctl snapshot restore '/backup/etcd-snapshot-latest.db' ; mv
/default.etcd/member/ /var/lib/etcd/
```

3. Antes de inicializar el clúster de Kubernetes, copie todos los certificados necesarios.
4. Cree el clúster con el `--ignore-preflight-errors=DirAvailable—var-lib-etcd` bandera.
5. Una vez que el clúster haya terminado, asegúrese de que los pods de kube-system hayan comenzado.
6. Utilice la `kubectl get crd` Comando para comprobar si existen los recursos personalizados que ha creado Trident y recuperar los objetos de Trident para garantizar que todos los datos estén disponibles.

## Recuperar la fecha utilizando snapshots de ONTAP

Las copias Snapshot tienen un papel importante al proporcionar opciones de recuperación a un momento específico para los datos de aplicaciones. Sin embargo, las copias Snapshot no son backups por sí mismas, no protegen contra fallos del sistema de almacenamiento u otras catástrofes. No obstante, son un método cómodo, rápido y sencillo para recuperar datos en la mayoría de escenarios. Obtenga más información sobre cómo usar la tecnología Snapshot de ONTAP para realizar backups del volumen y cómo restaurarlos.

- Si la política de snapshot no se ha definido en el back-end, de forma predeterminada utiliza el `none` política. Esto da como resultado que ONTAP no realice instantáneas automáticas. No obstante, el administrador de almacenamiento puede realizar copias Snapshot manuales o cambiar la política de Snapshot a través de la interfaz de gestión de ONTAP. Esto no afecta al funcionamiento de Trident.
- El directorio de instantáneas está oculto de forma predeterminada. De este modo se facilita la máxima compatibilidad de volúmenes aprovisionados mediante el `ontap-nas` y.. `ontap-nas-economy` de windows Habilite el `.snapshot` cuando utilice `ontap-nas` y.. `ontap-nas-economy` controladores para permitir que las aplicaciones recuperen datos de instantáneas directamente.
- Restaure un volumen a un estado registrado en una instantánea anterior mediante el `volume snapshot restore` Comando de la CLI de ONTAP. Al restaurar una copia Snapshot, la operación de restauración sobrescribe la configuración de volúmenes existente. Se perderán todos los cambios que se realicen en los datos del volumen después de crear la copia Snapshot.

```
cluster1::*> volume snapshot restore -vserver vs0 -volume vol3 -snapshot
vol3_snap_archive
```

## Replicación de datos mediante ONTAP

El replicación de datos puede tener un rol importante en la protección contra la pérdida de datos debido al fallo de la cabina de almacenamiento.

> Para obtener más información sobre las tecnologías de replicación de ONTAP, consulte "Documentación de ONTAP".

### Replicación de SnapMirror Storage Virtual Machines (SVM)

Puede utilizar "SnapMirror" Para replicar una SVM completa, que incluye su configuración y sus volúmenes. En caso de desastre, puede activar la SVM de destino de SnapMirror para empezar a servir datos. Puede volver al primario cuando se restauren los sistemas.

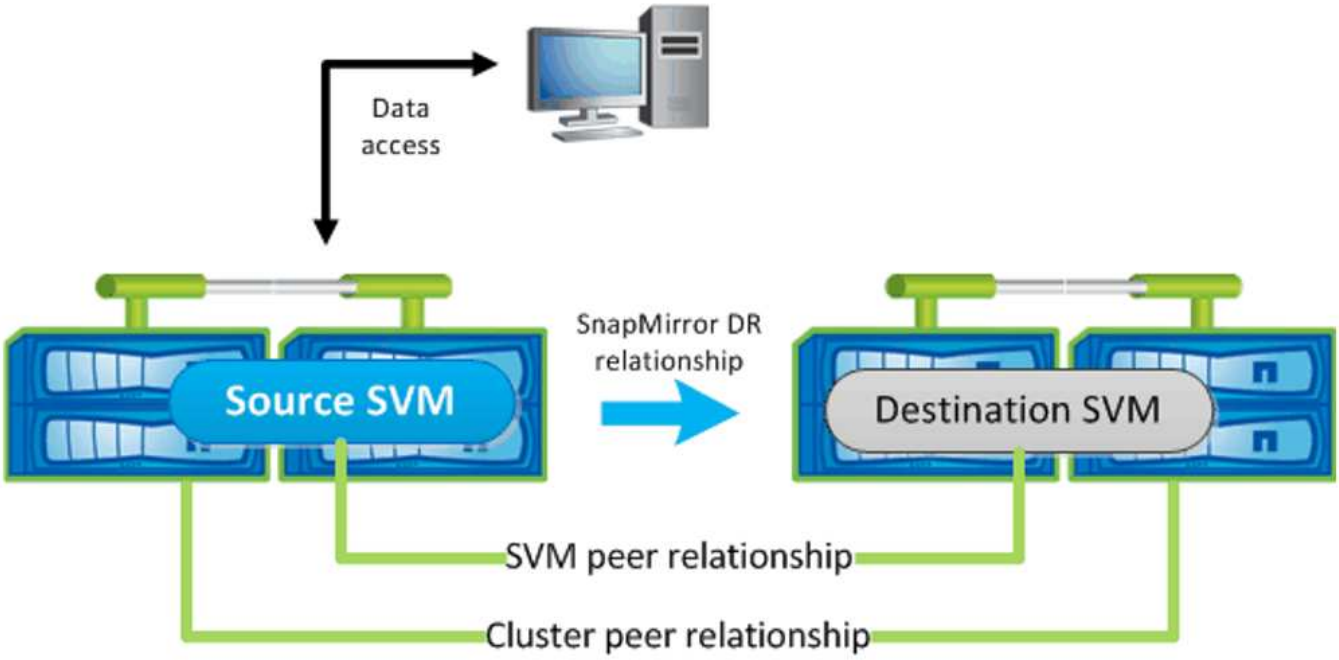
Astra Trident no puede configurar las relaciones de replicación por sí mismo, de modo que el administrador de almacenamiento pueda usar la función de replicación de SVM de SnapMirror de ONTAP para replicar automáticamente volúmenes en un destino de recuperación ante desastres (DR).

Tenga en cuenta lo siguiente si tiene pensado utilizar la función de replicación de SVM de SnapMirror o si actualmente utiliza la función:

- Debe crear un back-end distinto para cada SVM, la cual tiene habilitada la SVM-DR.
- Debe configurar las clases de almacenamiento para no seleccionar los back-ends replicados, excepto cuando se desee. Esto es importante para evitar que se aprovisionen volúmenes que no necesiten la protección de una relación de replicación en los back-end que sean compatibles con SVM-DR.
- Los administradores de aplicaciones deben comprender el coste y la complejidad adicionales que supone la replicación de datos, así como tener en cuenta un plan de recuperación antes de aprovechar esta replicación.
- Antes de activar la SVM de destino de SnapMirror, detenga todas las transferencias programadas de SnapMirror, aborte todas las transferencias continuas de SnapMirror, rompa la relación de replicación, detenga la SVM de origen e inicie la SVM de destino de SnapMirror.
- Astra Trident no detecta automáticamente fallos de SVM. Por lo tanto, en caso de que se produzca un error, el administrador debe ejecutar el `tridentctl backend update` Comando para activar la conmutación por error de Trident al nuevo back-end.

A continuación se ofrece información general de los pasos de configuración de SVM:

- Configure una relación entre iguales entre los clústeres de origen y destino y SVM.
- Cree la SVM de destino mediante el `-subtype dp-destination` opción.
- Cree un programa de trabajo de replicación para asegurarse de que la replicación se produce en los intervalos necesarios.
- Cree una replicación de SnapMirror a partir de la SVM de destino con la SVM de origen mediante el `-identity-preserve true` Opción para garantizar que las configuraciones de SVM de origen y las interfaces de SVM de origen se copian en el destino. En la SVM de destino, inicialice la relación de replicación de SVM de SnapMirror.




**Flujo de trabajo de recuperación ante desastres para Trident**

Astra Trident 19.07 y versiones posteriores utilizan los CRD de Kubernetes para almacenar y gestionar su propio estado. Usa los clústeres de Kubernetes `etcd` para almacenar sus metadatos. En este caso asumimos que el Kubernetes `etcd` Los archivos de datos y los certificados se almacenan en NetApp FlexVolume. Este volumen FlexVolume reside en una SVM, que tiene una relación de SVM-recuperación ante desastres de SnapMirror con una SVM de destino en el sitio secundario.

Los siguientes pasos describen cómo recuperar un único clúster Kubernetes maestro con Astra Trident en caso de desastre:

1. Si la SVM de origen falla, active la SVM de destino de SnapMirror. Para ello, debe detener las transferencias de SnapMirror programadas, anular las transferencias continuas de SnapMirror, romper la relación de replicación, detener la SVM de origen e iniciar la SVM de destino.
2. Desde la SVM de destino, monte el volumen que contiene Kubernetes `etcd` archivos de datos y certificados en el host que se configurarán como un nodo maestro.
3. Copie todos los certificados necesarios relacionados con el clúster de Kubernetes en `/etc/kubernetes/pki` y el etcd `member` archivos en `/var/lib/etcd`.
4. Cree un clúster de Kubernetes mediante el `kubeadm init` con el `--ignore-preflight -errors=DirAvailable—var-lib-etcd` bandera. Los nombres de host utilizados para los nodos de Kubernetes deben ser los mismos que el clúster de Kubernetes de origen.
5. Ejecute el `kubectl get crd` Comando para verificar si todos los recursos personalizados de Trident han aparecido y recuperar los objetos de Trident para verificar que todos los datos estén disponibles.
6. Actualice todos los back-ends necesarios para reflejar el nuevo nombre de SVM de destino. Para ello, ejecute el `./tridentctl update backend <backend-name> -f <backend-json-file> -n <namespace>` comando.

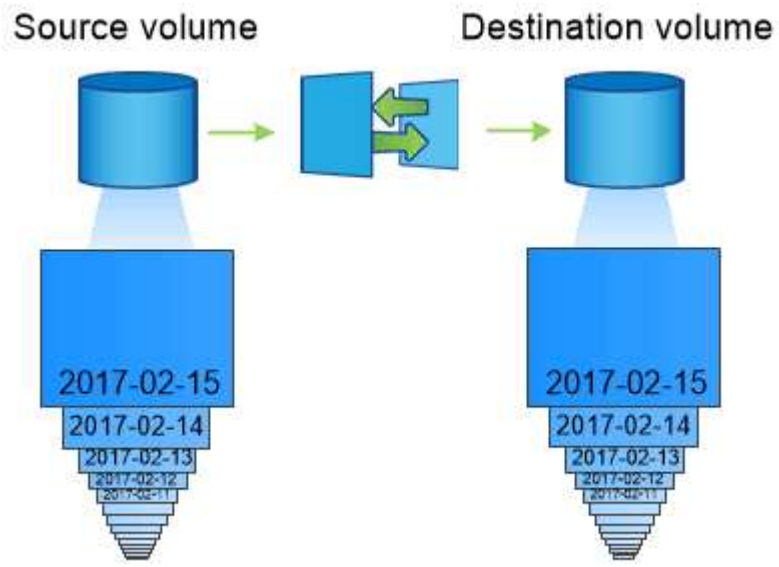
En el caso de los volúmenes persistentes de la aplicación, cuando se activa la SVM de destino, todos los volúmenes aprovisionados mediante Trident empiezan a servir datos. Una vez que el clúster de Kubernetes se configura en el lado de destino mediante los pasos descritos anteriormente, se inician todas las puestas en marcha y pods y las aplicaciones en contenedores deben ejecutarse sin ningún problema.

**Replicación de volúmenes de SnapMirror**

La replicación de volúmenes de SnapMirror de ONTAP es una función de recuperación ante desastres que permite llevar a cabo la conmutación al nodo de respaldo en el almacenamiento de destino desde el almacenamiento principal a nivel de volumen. SnapMirror crea una réplica o un reflejo de volumen del almacenamiento principal en el almacenamiento secundario mediante la sincronización de las copias Snapshot.

A continuación se ofrece información general de los pasos de configuración de la replicación de volúmenes de SnapMirror de ONTAP:

- Configure una relación entre los clústeres en los que residen los volúmenes y las SVM que sirven datos de los volúmenes.
- Cree una política de SnapMirror, que controla el comportamiento de la relación y especifica los atributos de configuración de esa relación.
- Cree una relación de SnapMirror entre el volumen de destino y el de origen mediante la[`snapmirror create` Command] y asigne la política de SnapMirror correspondiente.
- Una vez creada la relación de SnapMirror, inicialice la relación de forma que haya completado una transferencia inicial desde el volumen de origen al volumen de destino.




**Flujo de trabajo de recuperación ante desastres de volúmenes de SnapMirror para Trident**

En los siguientes pasos se describe cómo recuperar un único clúster Kubernetes maestro con Astra Trident.

1. En caso de desastre, detenga todas las transferencias programadas de SnapMirror y cancele todas las transferencias continuas de SnapMirror. Rompa la relación de replicación entre los volúmenes de destino y de origen para que el volumen de destino se convierta en de lectura/escritura.

2. Desde la SVM de destino, monte el volumen que contiene Kubernetes `etcd` archivos de datos y certificados en el host, que se configurarán como un nodo maestro.
3. Copie todos los certificados necesarios relacionados con el clúster de Kubernetes en `/etc/kubernetes/pki` y el etcd `member` archivos en `/var/lib/etcd`.
4. Ejecute el para crear un clúster de Kubernetes `kubeadm init` con el `--ignore-preflight -errors=DirAvailable—var-lib-etcd` bandera. Los nombres de host deben ser los mismos que el clúster de Kubernetes de origen.
5. Ejecute el `kubectl get crd` Comando para comprobar si todos los recursos personalizados de Trident han aparecido y recuperan objetos de Trident para garantizar que todos los datos estén disponibles.
6. Limpiar los back-ends anteriores y crear nuevos back-ends en Trident. Especifique el nuevo LIF de gestión, el nuevo nombre de la SVM y la contraseña de la SVM de destino.

#### Flujo de trabajo de recuperación ante desastres para volúmenes persistentes de aplicaciones

Los pasos siguientes describen cómo pueden ponerse volúmenes de destino de SnapMirror disponibles para cargas de trabajo en contenedores en caso de desastre:

1. Detenga todas las transferencias programadas de SnapMirror y cancele todas las transferencias continuas de SnapMirror. Rompa la relación de replicación entre el volumen de destino y el de origen para que el volumen de destino se convierta en de lectura/escritura. Borre las puestas en marcha que consumían PVC vinculado a volúmenes en la SVM de origen.
2. Una vez que el clúster de Kubernetes se ha configurado en el lado de destino mediante los pasos descritos anteriormente, limpie las puestas en marcha, las RVP y el VP, del clúster de Kubernetes.
3. Cree nuevos back-ends en Trident especificando las nuevas LIF de gestión y datos, el nuevo nombre de SVM y la contraseña de la SVM de destino.
4. Importe los volúmenes necesarios como un VP vinculado a una nueva RVP mediante la función de importación Trident.
5. Vuelva a poner en marcha las implementaciones de aplicaciones con las RVP recién creadas.

### Recuperar datos mediante copias de Snapshot de Element

Realizar un backup de los datos de un volumen de Element mediante la configuración de una programación de Snapshot para el volumen y la garantía de que las copias de Snapshot se tomen en los intervalos requeridos. Debe establecer la programación de Snapshot mediante las API o la interfaz de usuario de Element. Actualmente, no es posible establecer una programación de snapshots en un volumen a través del `solidfire-san` controlador.

En caso de que los datos se dañen, es posible seleccionar una snapshot determinada y revertir el volumen a la snapshot manualmente mediante las API o la interfaz de usuario de Element. De este modo se revierten los cambios que se hayan hecho al volumen desde el momento de la creación de la snapshot.

# Seguridad

## Seguridad

Utilice las recomendaciones que se enumeran aquí para asegurarse de que su instalación de Astra Trident es segura.

### Ejecute Astra Trident en su propio espacio de nombres

Es importante evitar que las aplicaciones, los administradores de aplicaciones, los usuarios y las aplicaciones de gestión accedan a las definiciones de objetos de Astra Trident o a los pods para garantizar un almacenamiento fiable y bloquear la potencial actividad maliciosa.

Para separar el resto de aplicaciones y usuarios de Astra Trident, instale siempre Astra Trident en su propio espacio de nombres Kubernetes (`trident`). Si coloca Astra Trident en su propio espacio de nombres, solo el personal administrativo de Kubernetes tiene acceso al pod de la Astra Trident y los artefactos (como los secretos CHAP y de back-end, si corresponde) almacenados en los objetos de CRD named. Debe asegurarse de permitir que solo los administradores tengan acceso al espacio de nombres de Astra Trident y, por lo tanto, tengan acceso a `tridentctl` cliente más.

### Utilice la autenticación CHAP con los back-ends DE SAN de ONTAP

Astra Trident admite la autenticación basada en CHAP para las cargas de trabajo SAN de ONTAP (mediante el `ontap-san` y.. `ontap-san-economy` de windows). NetApp recomienda utilizar CHAP bidireccional con Astra Trident para la autenticación entre un host y el back-end de almacenamiento.

En el caso de los back-ends de ONTAP que utilizan controladores de almacenamiento SAN, Astra Trident puede configurar CHAP bidireccional y gestionar los nombres de usuario y los secretos CHAP a través de `tridentctl`. Consulte "aquí" Para comprender cómo Astra Trident configura CHAP en los back-ends de ONTAP.

> La compatibilidad CON CHAP para los back-ends de ONTAP está disponible con Trident 20.04 y versiones posteriores.

### Utilice la autenticación CHAP con NetApp HCI y back-ends de SolidFire

NetApp recomienda poner en marcha CHAP bidireccional para garantizar la autenticación entre un host y los back-ends de NetApp HCI y SolidFire. Astra Trident utiliza un objeto secreto que incluye dos contraseñas CHAP por inquilino. Cuando Trident se instala como aprovisionador CSI, gestiona los secretos CHAP y los almacena en un `tridentvolume` Objeto CR para el PV correspondiente. Cuando se crea un VP, CSI Astra Trident utiliza los secretos CHAP para iniciar una sesión iSCSI y comunicarse con el sistema NetApp HCI y SolidFire a través de CHAP.

> Los volúmenes creados por CSI Trident no están asociados con ningún grupo de acceso de volúmenes.

En el frontend que no sea CSI, Kubernetes gestiona la conexión de volúmenes como dispositivos en los nodos de trabajo. Tras crear un volumen, Astra Trident realiza una llamada API al sistema HCI/SolidFire de NetApp para recuperar los secretos si ese secreto no existe ya. A continuación, Astra Trident pasa los secretos a Kubernetes. La kuelet que se encuentra en cada nodo accede a los secretos a través de la API de Kubernetes y los utiliza para ejecutar y habilitar CHAP entre cada nodo que accede al volumen y el sistema HCI/SolidFire de NetApp donde están ubicados los volúmenes.

### Utilice Astra Trident con NVE y NAE

ONTAP de NetApp proporciona cifrado de datos en reposo para proteger los datos confidenciales en el caso de robo, devolución o reasignación de un disco. Para obtener más información, consulte "Configure la información general de cifrado de volúmenes de NetApp".

- Si NAE está habilitado en el back-end, cualquier volumen aprovisionado en Astra Trident se habilitará para NAE.

- Si NAE no está habilitado en el back-end, todos los volúmenes aprovisionados en Astra Trident tendrán el cifrado NVE habilitado a menos que establezca el indicador NVE en `false` en la configuración de back-end.

> Los volúmenes que se crean en Astra Trident en un back-end con la NAE habilitada deben ser NVE o NAE cifrados.
>
> - Puede establecer el indicador NVE Encryption como `true` En la configuración del back-end de Trident, con el fin de anular el cifrado NAE y utilizar una clave de cifrado específica por volumen.
> - Establecer la Marca NVE Encryption como `false` En un back-end habilitado para NAE se creará un volumen habilitado para NAE. No puede deshabilitar el cifrado NAE mediante la Marca NVE Encryption a. `false`.

- Es posible crear manualmente un volumen NVE en Astra Trident mediante la definición explícita de la Marca NVE a. `true`.

Para obtener más información sobre las opciones de configuración del back-end, consulte:

- "Opciones de configuración DE SAN de ONTAP"
- "Opciones de configuración de NAS de ONTAP"

## Configuración de clave unificada de Linux (LUKS)

Puede habilitar Unified Key Setup (LUKS) de Linux para cifrar los volúmenes DE ECONOMÍA SAN de ONTAP y SAN DE ONTAP en Astra Trident. Astra Trident admite la rotación de claves de acceso y la expansión de volumen para volúmenes cifrados con LUKS.

En Astra Trident, los volúmenes cifrados por LUKS utilizan el cifer y el modo AES-xts-Capellanía, como recomienda "NIST".

#### Antes de empezar

- Los nodos de trabajo deben tener instalado cryptsetup 2.1 o superior (pero inferior a 3.0). Si desea más información, visite "Gitlab: Cryptsetup".
- Por motivos de rendimiento, recomendamos que los nodos de trabajo admitan las nuevas instrucciones estándar de cifrado avanzado (AES-ni). Para verificar el soporte de AES-ni, ejecute el siguiente comando:

  ```
  grep "aes" /proc/cpuinfo
  ```

  Si no se devuelve nada, su procesador no admite AES-ni. Para obtener más información sobre AES-ni, visite: "Intel: Instrucciones estándar de cifrado avanzado (AES-ni)".

#### Active el cifrado LUKS

Puede habilitar el cifrado por volumen en el lado del host usando la configuración de clave unificada de Linux (LUKS) para SAN de ONTAP y volúmenes DE ECONOMÍA SAN de ONTAP.

#### Pasos

1. Defina los atributos de cifrado LUKS en la configuración de backend. Para obtener más información sobre las opciones de configuración del back-end para SAN de ONTAP, consulte "Opciones de configuración DE SAN de ONTAP".

```
"storage": [
    {
        "labels":{"luks": "true"},
        "zone":"us_east_1a",
        "defaults": {
            "luksEncryption": "true"
        }
    },
    {
        "labels":{"luks": "false"},
        "zone":"us_east_1a",
        "defaults": {
            "luksEncryption": "false"
        }
    },
]
```

2. Uso `parameters.selector` Para definir los pools de almacenamiento mediante el cifrado LUKS. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: netapp.io/trident
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

3. Cree un secreto que contenga la frase de paso LUKS. Por ejemplo:

```
kubectl -n trident create -f luks-pvc1.yaml
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: A
  luks-passphrase: secretA
```

#### Limitaciones

Los volúmenes cifrados LUKS no pueden aprovechar la deduplicación y la compresión de ONTAP.

### Gire una frase de paso LUKS

Puede girar la frase de paso de LUKS y confirmar la rotación.

> No olvide una clave de acceso hasta que haya verificado que ya no hace referencia a ningún volumen, snapshot o secreto. Si se pierde una clave de acceso de referencia, es posible que no se pueda montar el volumen y los datos seguirán estando cifrados e inaccesibles.

#### Acerca de esta tarea

LA rotación DE la frase de paso LUKS se produce cuando se crea un pod que monta el volumen después de especificar una nueva frase de paso LUKS. Cuando se crea un nuevo pod, Astra Trident compara la frase de paso de LUKS del volumen con la frase de paso activa en el secreto.

- Si la clave de acceso del volumen no coincide con la clave de acceso activa en el secreto, se produce la rotación.
- Si la clave de acceso del volumen coincide con la clave de acceso activa en el secreto, el `previous-luks-passphrase` se ignora el parámetro.

#### Pasos

1. Añada el `node-publish-secret-name` y.. `node-publish-secret-namespace` Parámetros de StorageClass. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-san
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/backendType: "ontap-san"
  csi.storage.k8s.io/node-stage-secret-name: luks
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-publish-secret-name: luks
  csi.storage.k8s.io/node-publish-secret-namespace: ${pvc.namespace}
```

2. Identifique las bases de datos passhrases existentes en el volumen o la snapshot.

   **Volumen**

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["A"]
```

**Snapshot**

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["A"]
```

3. Actualice el secreto LUKS del volumen para especificar las passphrases nuevas y anteriores. Asegúrese `previous-luke-passphrase-name` y.. `previous-luks-passphrase` coincidir con la frase de contraseña anterior.

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

4. Cree un nuevo pod montando el volumen. Esto es necesario para iniciar la rotación.
5. Compruebe que se ha girado la frase de paso.

**Volumen**

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["B"]
```

**Snapshot**

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["B"]
```

**Resultados**

La frase de contraseña se giró cuando solo se devuelve la nueva frase de contraseña en el volumen y la instantánea.

> Si se devuelven dos passphrasas, por ejemplo `luksPassphraseNames: ["B", "A"]`, la rotación está incompleta. Puede activar un nuevo pod para intentar completar la rotación.

### Habilite la expansión de volumen

Es posible habilitar la ampliación de volumen en un volumen cifrado LUKS.

#### Pasos

1. Habilite el `CSINodeExpandSecret` puerta de características (beta 1.25+). Consulte "Kubernetes 1.25: Use Secrets for Node-Driven Expansion of CSI Volumes" para obtener más detalles.
2. Añada el `node-expand-secret-name` y.. `node-expand-secret-namespace` Parámetros de StorageClass. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: netapp.io/trident
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-expand-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-expand-secret-namespace: ${pvc.namespace}
allowVolumeExpansion: true
```

#### Resultados

Al iniciar la ampliación de almacenamiento en línea, el kubelet pasa las credenciales adecuadas al controlador.